УТЕЧКА ДАННЫХ КАК АКТУАЛЬНАЯ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРИЧИНЫ ВОЗНИКНОВЕНИЯ, ПОСЛЕДСТВИЯ И МЕТОДЫ ПРЕДОТВРАЩЕНИЯ

Карабаев Рустам Зафарович

Ташкентский университет информационных технологий имени Мухаммада аль-Хорезмий

Магистрант 2-го курса факультета Цифровой экономики

ORCID: 0009-0008-7487-2385

Рахимов Мухаммад Абдурахмон угли

ГУ «Центр кибербезопасности»

Главный специалист информационно-аналитического отдела

ORCID: 0009-0006-6977-4954

Аннотация. В статье рассматривается проблема утечки данных как одна из наиболее актуальных угроз современной информационной безопасности. Анализируются основные причины возникновения инцидентов, связанные с человеческим фактором, недостаточной защищённостью информационных систем, вредоносным программным обеспечением, фишинговыми атаками и неправильной организацией процессов хранения и обработки информации. Особое внимание уделяется последствиям утечки конфиденциальных сведений для государственных органов, коммерческих организаций и физических лиц. Рассматриваются современные методы предотвращения утечек данных, включая шифрование информации, многофакторную аутентификацию, разграничение прав доступа, системы предотвращения потери данных (DLP), мониторинг информационных систем, резервное копирование и повышение уровня киберграмотности сотрудников. Обосновывается необходимость комплексного подхода к обеспечению информационной безопасности, объединяющего технические, организационные и правовые меры защиты. Дополнительно рассматриваются нормативно-правовая база Республики Узбекистан в сфере защиты персональных данных и кибербезопасности, инциденты 2026 года, а также возможности поведенческой аналитики (UEBA) и искусственного интеллекта для раннего выявления утечек.

Ключевые слова: утечка данных, информационная безопасность, кибербезопасность, конфиденциальная информация, защита персональных данных, DLP, шифрование, кибератаки, управление доступом, предотвращение утечек, UEBA.

Annotatsiya. Ushbu maqolada ma’lumotlarning sizib chiqishi zamonaviy axborot xavfsizligining eng dolzarb tahdidlaridan biri sifatida ko‘rib chiqiladi. Ma’lumotlar sizib chiqishiga sabab bo‘luvchi asosiy omillar, jumladan, inson omili, axborot tizimlarining yetarli darajada himoyalanmaganligi, zararli dasturiy ta’minot, fishing hujumlari hamda axborotni saqlash va qayta ishlash jarayonlaridagi kamchiliklar tahlil qilinadi. Shuningdek, maxfiy ma’lumotlarning oshkor bo‘lishi davlat organlari, tijorat tashkilotlari va jismoniy shaxslar faoliyatiga ko‘rsatadigan salbiy ta’siri yoritiladi. Maqolada ma’lumotlar sizib chiqishining oldini olish bo‘yicha zamonaviy usullar, jumladan, ma’lumotlarni shifrlash, ko‘p faktorli autentifikatsiya, foydalanish huquqlarini cheklash, ma’lumotlar yo‘qolishining oldini olish tizimlari (DLP), axborot tizimlarini monitoring qilish, zaxira nusxalarini yaratish va xodimlarning kiberxavfsizlik savodxonligini oshirish masalalari ko‘rib chiqiladi. Bundan tashqari, O‘zbekiston Respublikasining shaxsga doir ma’lumotlar va kiberxavfsizlik sohasidagi qonunchiligi, 2026-yilgi hodisalar hamda sizib chiqishni erta aniqlashda xulq-atvor tahlili (UEBA) va sun’iy intellekt imkoniyatlari ko‘rib chiqiladi.

Kalit so‘zlar: ma’lumotlar sizib chiqishi, axborot xavfsizligi, kiberxavfsizlik, maxfiy axborot, shaxsiy ma’lumotlarni himoya qilish, DLP, shifrlash, kiberhujumlar, kirish huquqlarini boshqarish, ma’lumotlar sizib chiqishining oldini olish, UEBA.

Abstract. This article examines data leakage as one of the most significant threats to modern information security. It analyzes the primary causes of data breaches, including human error, insufficient protection of information systems, malicious software, phishing attacks, and inadequate information storage and processing practices. Particular attention is paid to the consequences of confidential information disclosure for government institutions, commercial organizations, and individuals. The article explores modern data leakage prevention methods, including data encryption, multi-factor authentication, access control, Data Loss Prevention (DLP) systems, information system monitoring, backup procedures, and employee cybersecurity awareness training. It emphasizes the importance of an integrated approach to information security that combines technical, organizational, and legal protection measures. In addition, the article considers the legal framework of the Republic of Uzbekistan on personal data protection and cybersecurity, incidents reported in 2026, and the potential of user and entity behavior analytics (UEBA) and artificial intelligence for early leak detection.

Key words: data leakage, information security, cybersecurity, confidential information, personal data protection, DLP, encryption, cyberattacks, access control, data loss prevention, UEBA.

Введение. В условиях стремительной цифровизации экономики, государственного управления и общественных отношений информация становится одним из наиболее ценных ресурсов современного общества. Государственные учреждения, коммерческие организации и частные лица ежедневно используют информационные системы для хранения, обработки и передачи значительных объёмов данных. Развитие цифровых технологий способствует

повышению эффективности деятельности организаций, однако одновременно увеличивает риски нарушения конфиденциальности информации.

Одной из наиболее серьёзных угроз в данной области является утечка данных. Под утечкой данных понимается несанкционированное раскрытие, передача, копирование или распространение информации за пределы установленной системы доступа. Она может происходить как вследствие целенаправленных кибератак, так и из-за случайных ошибок сотрудников, недостатков технической защиты или неправильной организации процессов обработки информации.

Актуальность данной проблемы подтверждается международными исследованиями. Согласно отчёту Verizon Data Breach Investigations Report за 2025 год, в рамках исследования было рассмотрено 22 052 инцидента информационной безопасности, включая 12 195 подтверждённых случаев утечки данных. В отчёте также отмечается увеличение участия третьих сторон в инцидентах до 30% и рост эксплуатации уязвимостей на 34% [9].

Проблема актуальна и для Республики Узбекистан. По данным службы UZCERT, в 2025 году на веб-сайтах выявлено 247 событий кибербезопасности, на веб-ресурсах – более 700 уязвимостей, устранено свыше 67 миллионов кибератак [15]. В период с 27 по 30 января 2026 года кибератакам подверглись информационные системы трёх государственных ведомств, в результате чего, по заявлению министра цифровых технологий, было распространено около 60 тысяч единиц персональных данных [16].

В связи с этим предотвращение утечек информации должно рассматриваться не только как техническая задача IT-подразделений, но и как комплексное направление управления информационной безопасностью организации.

Литературный обзор. Проблема защиты конфиденциальной информации и предотвращения утечек данных рассматривается в научной литературе, международных стандартах и методических документах ведущих организаций в области кибербезопасности.

Одним из значимых источников в данной области является публикация Национального института стандартов и технологий США (NIST) - Special Publication 1800-29 «Data Confidentiality: Detect, Respond to, and Recover from Data Breaches», опубликованная в 2024 году. В документе рассматриваются подходы к выявлению, реагированию и восстановлению после инцидентов, связанных с нарушением конфиденциальности информации. Авторы подчёркивают необходимость применения комплексных механизмов защиты, обеспечивающих контроль информационных активов и своевременное обнаружение инцидентов [1].

Важное значение для исследования имеет также NIST Special Publication 800-61 Revision 3, опубликованная в апреле 2025 года. Документ посвящён рекомендациям по управлению инцидентами информационной безопасности и интеграции процессов реагирования в общую систему управления киберрисками организации. В нём рассматривается необходимость подготовки к инцидентам, их выявления, реагирования и восстановления деятельности [2].

Дополнительным источником является ежегодный отчёт Verizon Data Breach Investigations Report (DBIR). Данное исследование позволяет оценить актуальные тенденции в области киберугроз на основании анализа реальных инцидентов. В отчёте за 2025 год особое внимание уделяется компрометации учётных данных, эксплуатации уязвимостей и рискам, связанным с участием сторонних организаций [9].

Отдельное направление исследований связано с управлением информационной безопасностью на основе международных стандартов ISO/IEC 27001 и ISO/IEC 27002. Стандарт ISO/IEC 27001 определяет требования к системе менеджмента информационной безопасности, а ISO/IEC 27002 содержит рекомендации по применению организационных и технических мер защиты информации. Их использование позволяет организациям систематизировать управление рисками, определить ответственность сотрудников и сформировать комплексную систему контроля информационных активов [3, 4].

Экономические последствия утечек и роль средств автоматизации отражены в отчёте IBM и Ponemon Institute «Cost of a Data Breach Report 2025»: средняя стоимость одной утечки в мире составила 4,44 млн долларов США, а организации, широко применяющие искусственный интеллект и автоматизацию в процессах безопасности, сокращали ущерб в среднем на 1,9 млн долларов и жизненный цикл инцидента – на 80 дней [10]. Возможности и ограничения методов глубокого обучения при выявлении внутренних нарушителей по данным о поведении пользователей систематизированы в обзоре Ш. Юаня и С. Ву [11].

В Республике Узбекистан правовую основу защиты данных образуют Закон «О персональных данных», обязывающий собственника и оператора обеспечивать целостность, сохранность и конфиденциальность персональных данных [12], и Закон «О кибербезопасности», который определяет уполномоченный государственный орган и формы принятия мер в отношении инцидентов кибербезопасности [13]. Указом Президента от 10 марта 2026 года утверждена Стратегия кибербезопасности на 2026–2030 годы, в числе задач которой – совершенствование законодательства и внедрение стандартов в области защиты данных [14].

Отдельный пласт литературы посвящён безопасности промышленных систем управления, где утечка технологических данных и учётных записей создаёт риски не только для конфиденциальности информации, но и для непрерывности производственных процессов.

Что касается атак и попыток взлома кибер-инфраструктуры в частных компаниях и промышленных предприятиях, то можно отметить, что в настоящее время на промышленных предприятиях для управления производственными процессами и их автоматизации широко используются сети OT (Operational Technology) и ICS (Industrial Control Systems). Интеграция этих систем с корпоративными и внешними сетями делает их уязвимыми для различных киберугроз. Необычная сетевая активность в среде OT/ICS, неожиданные соединения между устройствами или изменения в управляющих командах могут свидетельствовать о наличии потенциальной угрозы. Поэтому своевременное обнаружение аномальной активности и оценка степени её опасности имеют важное значение. В контексте настоящего исследования

это означает, что меры предотвращения утечек должны охватывать не только корпоративные информационные системы, но и технологические сети.

Труд Эрика Д. Кнаппа и Джоэла Т. Лэнгилла «Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems» является по сути одним из самых важных источников информации по безопасности промышленных сетей. В книге проанализированы специфическая сетевая архитектура, протоколы, приложения и требования безопасности ICS, SCADA и других промышленных систем управления. Авторы показывают, что для защиты промышленных сетей недостаточно напрямую применять обычные подходы IT-безопасности - необходимо учитывать особенности среды OT/ICS [22].

А в работе «Guide to Industrial Control Systems (ICS) Security», подготовленной Китом А. Стоуффером, Викторией Ю. Пиллитери, Сюзанной Лайтман, Маршаллом Абрамсом и Адамом Ханом, предлагается комплексный подход к обеспечению безопасности ICS в рамках NIST SP 800-82. По данным NIST, эта работа направлена на определение мер безопасности с учётом угроз, уязвимостей и рисков в среде ICS [24].

В подходе Кита Стоуффера подчёркивается, что при обеспечении безопасности ICS необходимо совместно учитывать эффективность работы систем, их надёжность и требования безопасности. Согласно этому подходу, обеспечение безопасности промышленных систем управления требует не простого применения стандартов, предназначенных для IT-систем, а их адаптации к среде ICS.

В работе Ширли М. Радак «Protecting Industrial Control Systems – Key Components of Our Nation's Critical Infrastructures» освещаются роль ICS в составе критической инфраструктуры, их угрозы и уязвимости, а также вопросы управления рисками. Опираясь на концепцию NIST SP 800-82, автор подчёркивает необходимость применения в безопасности ICS риск-ориентированного подхода (risk-based approach) [25].

По мнению Радак, прежде чем выбирать меры безопасности, необходимо оценить существующие в системе угрозы, уязвимости и их возможные последствия.

В третьем издании книги Эрика Д. Кнаппа «Industrial Network Security», вышедшем в 2024 году, расширено рассмотрение уязвимостей современных сетей ICS, мер безопасности, протоколов SCADA, оценки промышленных сетей и вопросов, связанных со стандартами, такими как ISA/IEC 62443 [23].

Методология исследования. В ходе исследования проведён анализ научной литературы, международных стандартов ISO/IEC 27001, ISO/IEC 27002 и рекомендаций NIST. Методом классификации определены основные причины утечек данных, включая человеческий фактор, технические уязвимости, внешние кибератаки, недостатки управления доступом и риски сторонних поставщиков, а также неконтролируемое использование сервисов искусственного интеллекта. Сравнительный анализ использован для оценки функциональных возможностей DLP, SIEM, EDR, MFA, шифрования и RBAC. На основе полученных результатов разработана

пятиуровневая модель предотвращения утечек данных, объединяющая организационные, технические и аналитические меры защиты информации. Дополнительно изучены нормативно-правовые акты Республики Узбекистан в сфере персональных данных и кибербезопасности, официальная статистика и сообщения открытых источников об инцидентах 2026 года; сведения, не получившие официального подтверждения, приводятся с соответствующей оговоркой.

Результат исследования. В результате проведённого анализа определены основные факторы возникновения утечек данных, рассмотрены возможности современных средств защиты и разработана комплексная модель предотвращения несанкционированного раскрытия информации.

Классификация основных причин утечек данных

На основании изученных источников причины возникновения утечек были систематизированы по шести основным категориям.

Таблица 1

Категория	**Основные причины**	**Возможные последствия**
Человеческий фактор	Ошибки сотрудников, фишинг, нарушение правил работы с данными	Случайное или намеренное раскрытие информации
Технические уязвимости	Устаревшее ПО, ошибки конфигурации, отсутствие обновлений	Несанкционированный доступ к системам
Внешние кибератаки	Компрометация учётных записей, вредоносное ПО	Кража и распространение данных
Недостатки управления доступом	Избыточные привилегии, отсутствие контроля пользователей	Доступ к информации неуполномоченных лиц
Сторонние поставщики	Недостаточная защищённость подрядчиков и облачных сервисов	Компрометация информации через внешнюю инфраструктуру
Неконтролируемое использование ИИ-сервисов	Передача служебных данных во внешние ИИ-сервисы без согласования («теневой ИИ»),	Раскрытие персональных данных и интеллектуальной собственности, рост ущерба от инцидента

	отсутствие политик использования ИИ	

Полученные результаты показывают, что проблема утечки данных не может рассматриваться исключительно как результат внешних кибератак. Существенное значение имеют внутренние процессы организации, включая управление доступом, контроль действий сотрудников и обеспечение безопасности сторонних сервисов.

Шестая категория отражает сравнительно новый фактор: по данным IBM, каждая пятая организация столкнулась с утечкой, связанной с несанкционированным использованием сотрудниками ИИ-сервисов, при этом у 63% организаций отсутствовали политики управления искусственным интеллектом [10].

Актуальность предложенной классификации подтверждают события последних месяцев.

Развитие информационных технологий не только обеспечивает стремительные мировые технологические прорывы. Оно также является источником появления новых угроз для цифровой безопасности не только отдельных граждан или компаний, но и также зачастую всей государственной системы управления страной или группой стран.

За октябрь-ноябрь 2026 года, как в мировых средствах массовой информации, так и в специализированных изданиях появилось множество сообщений о серии взломов и хищений средств.

Пожалуй, самыми громкими новостями стали взлом криптовалютной биржи BINANCE и выявление критических уязвимостей в PHP – популярном серверном скриптовом языке программирования, созданном специально для веб-разработки и создания динамических сайтов.

В результате взлома криптовалютной биржи BINANCE злоумышленники вывели цифровые активы на сумму примерно 6,4 миллиарда долларов США, что стало крупнейшей кражей в истории криптоиндустрии [17]. Взлом произошёл 29 октября 2026 года; по оценке аналитической компании Chainalysis, за ним стоит связанная с КНДР группировка TraderTraitor [17], а отправной точкой атаки, по сообщениям СМИ, стала компрометация рабочей среды разработчика.

Суть инцидента с PHP заключалась в выявлении двух критических уязвимостей (CVE-2026-109618 и CVE-2026-109619), затрагивающих PHP начиная с версии 5.4: в результате ошибок класса Use-After-Free в ядре PHP неаутентифицированный злоумышленник получал возможность выполнять произвольный код на сервере [18]. Исправления вышли 21 октября 2026 года, на следующий день после утечки сведений об уязвимостях; до их установки рекомендовалось ограничивать доступ к уязвимым сервисам вплоть до их временной

изоляции. По оценке компании Palo Alto Networks, потенциально уязвимыми были более 22 миллионов доступных из Интернета экземпляров PHP [19].

При этом уязвимости, получившие название PHP2Shell, были обнаружены исследователями с применением инструментов искусственного интеллекта [19]; это объясняет, почему они оставались ненайденными в коде более десяти лет. Подтверждений того, что оба инцидента были звеньями одной цепи, в открытых источниках нет, однако они показывают, что искусственный интеллект ускоряет поиск уязвимостей как для специалистов по защите, так и для злоумышленников.

Также в этот период в Узбекистане стала резонансной новость о возможной утечке в Интернет персональных данных более 27 миллионов граждан страны. В качестве доказательства хакерская группировка Butterfly, заявившая о взломе, опубликовала сведения, представленные как персональные данные министра цифровых технологий Узбекистана Шерзода Шерматова (дата рождения, номер телефона и персональный номер гражданина Узбекистана) [20]. Однако уже через несколько дней представители группировки опровергли факт публикации базы данных и заявили лишь об обнаружении уязвимостей в государственных информационных системах; независимого подтверждения утечки в открытых источниках на момент подготовки статьи нет [21].

Даже если подобная утечка имела место, несомненно, что помимо версий о человеческом факторе, имеет право на жизнь версия о причастности к возможному инциденту использования нейросетей и искусственного интеллекта – как минимум в качестве инструментария злоумышленников.

Сопоставление этих событий с таблицей 1 показывает, что в каждом из них проявилось сразу несколько категорий причин: в инциденте с Binance – человеческий фактор и компрометация сторонних инструментов разработки, в случае PHP2Shell – техническая уязвимость широко распространённого программного компонента, а сообщения об утечке данных граждан Узбекистана показывают, насколько важно проверять подобные заявления до официального подтверждения.

Сравнительный анализ современных методов предотвращения утечек

Для определения наиболее целесообразных механизмов защиты проведено сравнение основных технологий, применяемых в современных информационных системах.

Таблица 2

Технология	**Основная функция**	**Роль в предотвращении утечек**
DLP	Контроль движения конфиденциальных данных	Выявление и блокирование запрещённой передачи

SIEM	Сбор и анализ событий безопасности	Обнаружение подозрительной активности
EDR	Выявление угроз на конечных устройствах	Обнаружение вредоносной активности и реагирование
MFA	Многофакторная проверка пользователя	Снижение риска компрометации учётных записей
Шифрование	Защита содержимого информации	Снижение риска раскрытия данных при получении доступа к носителю
RBAC	Ролевое управление доступом	Ограничение доступа в соответствии с обязанностями
Backup	Резервное копирование	Восстановление информации после инцидента
UEBA	Поведенческая аналитика пользователей и сущностей	Раннее выявление аномальных действий сотрудников и скомпрометированных учётных записей

Сравнительный анализ показывает, что перечисленные технологии выполняют различные, но взаимодополняющие функции. Например, шифрование обеспечивает защиту содержимого данных, DLP контролирует их передачу, а SIEM позволяет выявлять взаимосвязанные события безопасности.

Следовательно, наиболее эффективным решением является не использование одной отдельной технологии, а их интеграция в общую систему информационной безопасности.

Особое место среди рассмотренных технологий занимает поведенческая аналитика пользователей и сущностей (UEBA). Такие системы на основе журналов событий формируют профиль обычного поведения каждого пользователя, учётной записи и устройства, а затем статистическими методами и методами машинного обучения оценивают отклонения от этого профиля. Признаками готовящейся утечки могут служить массовая выгрузка документов, обращение к данным в нетипичное время, доступ к ресурсам, не связанным с должностными обязанностями, а также передача файлов на внешние адреса.

Преимущество такого подхода состоит в том, что он позволяет выявлять действия легитимных пользователей и скомпрометированных учётных записей, которые не нарушают формальных правил DLP и SIEM. Вместе с тем исследователи указывают на ограничения метода: крайне малую долю вредоносных действий в общем потоке событий, недостаток размеченных данных, способность нарушителя подстраиваться под модель и сложность объяснения её

решений [11]. Поэтому результаты UEBA следует рассматривать как основание для проверки специалистом, а не как окончательный вывод.

Искусственный интеллект при этом выступает и фактором риска: по данным отчёта IBM, в 16% утечек злоумышленники сами применяли ИИ, главным образом для фишинга, а 97% организаций, сообщивших об инцидентах с ИИ-системами, не имели надлежащих средств управления доступом к ним [10].

Разработка комплексной модели предотвращения утечек данных

На основании результатов исследования предлагается пятиуровневая модель защиты информации.

1)Первый уровень - организационный контроль.

Предусматривает разработку политик информационной безопасности, классификацию данных, определение ответственных лиц и установление правил работы с конфиденциальной информацией.

2)Второй уровень - техническая защита.

Включает применение DLP, SIEM, EDR, MFA, шифрования, межсетевых экранов и механизмов управления доступом.

3)Третий уровень - аналитический мониторинг.

Предусматривает постоянный анализ событий информационной безопасности, выявление аномального поведения пользователей и контроль операций с конфиденциальными данными. Технологической основой данного уровня выступают системы SIEM и UEBA.

4)Четвёртый уровень - человеческий фактор.

Включает повышение киберграмотности сотрудников, обучение распознаванию фишинговых сообщений и формирование культуры ответственного обращения с информацией.

5)Пятый уровень - реагирование и восстановление.

Предполагает наличие плана реагирования на инциденты, проведение расследований, устранение причин утечки и восстановление нормальной деятельности организации.

Все пять уровней должны функционировать как единая система, обеспечивающая непрерывный контроль состояния информационной безопасности.

Применительно к Республике Узбекистан каждый уровень модели опирается на действующие нормативные требования. Организационный и технический уровни соответствуют обязанности собственника и оператора обеспечивать целостность, сохранность и конфиденциальность персональных данных и предотвращать их незаконную обработку [12]. Пятый уровень согласуется с предусмотренными Законом «О кибербезопасности» формами

принятия мер в отношении инцидентов, включая предоставление сведений о них правоохранительным органам [13]. Стратегия кибербезопасности на 2026–2030 годы дополнительно предусматривает проведение конкурсов по выявлению уязвимостей государственных информационных систем с участием независимых экспертов [14], что усиливает третий уровень модели внешней проверкой. Таким образом, нормативно-правовое обеспечение выступает сквозным основанием всех пяти уровней.

Заключение. В результате проведённого исследования установлено, что утечка данных представляет собой комплексную угрозу информационной безопасности, способную оказывать существенное влияние на финансовую, операционную и репутационную устойчивость государственных и коммерческих организаций.

Анализ научной литературы и международных методических документов позволил определить, что основные причины утечек связаны с человеческим фактором, техническими уязвимостями, недостатками управления доступом, внешними кибератаками и рисками, возникающими при взаимодействии со сторонними поставщиками услуг, а также с неконтролируемым использованием сервисов искусственного интеллекта.

Проведённое сравнение современных технологий показало, что DLP, SIEM, EDR, MFA, шифрование и ролевое управление доступом выполняют взаимодополняющие функции. Их интеграция позволяет обеспечить более эффективный контроль над конфиденциальной информацией на различных этапах её хранения, обработки и передачи.

В рамках исследования предложена пятиуровневая модель предотвращения утечек данных, включающая организационный контроль, техническую защиту, аналитический мониторинг, управление человеческим фактором, реагирование и восстановление. Данная модель может быть адаптирована к особенностям информационной инфраструктуры различных организаций.

Отдельно установлено, что применение искусственного интеллекта и методов статистического анализа создаёт дополнительные возможности для выявления аномальной активности пользователей и раннего обнаружения потенциальных инцидентов. Вместе с тем такие технологии должны применяться в сочетании с традиционными средствами защиты и экспертной оценкой специалистов.

Применительно к Республике Узбекистан показано, что предложенная модель согласуется с требованиями Законов «О персональных данных» и «О кибербезопасности» и задачами Стратегии кибербезопасности на 2026–2030 годы. Анализ инцидентов 2026 года подтверждает, что сообщения об утечках требуют проверки, а их причины, как правило, сочетают несколько категорий предложенной классификации.

Научно-практическая значимость исследования заключается в систематизации причин возникновения утечек, сравнительной оценке современных механизмов защиты и разработке комплексной модели предотвращения несанкционированного раскрытия информации.

Перспективы дальнейших исследований связаны с практической апробацией предложенной модели, оценкой эффективности интеграции DLP и SIEM, а также разработкой интеллектуальных алгоритмов выявления аномального поведения пользователей в корпоративных информационных системах.

Таким образом, предотвращение утечек данных должно рассматриваться как непрерывный процесс управления информационными рисками, требующий сочетания современных технологий, организационной дисциплины и постоянного повышения уровня киберграмотности персонала.

Список использованной литературы

1. Fisher W., Craft R. E., Ekstrom M., Sexton J., Sweetnam J. Data Confidentiality: Detect, Respond to, and Recover from Data Breaches. NIST Special Publication 1800-29. - National Institute of Standards and Technology, 2024.
2. Nelson A., Rekhi S., Scarfone K., Souppaya M. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST Special Publication 800-61 Revision 3. - NIST, 2025.
3. International Organization for Standardization. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. - Geneva: ISO, 2022.
4. International Organization for Standardization. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls. - Geneva: ISO, 2022.
5. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. - NIST, 2024.
6. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5. - NIST, 2020 (с последующими обновлениями).
7. Cybersecurity and Infrastructure Security Agency. Implementing Phishing-Resistant MFA. - CISA.
8. National Institute of Standards and Technology. Incident Response Project. - NIST.
9. Verizon. 2025 Data Breach Investigations Report. - Verizon Business, 2025.
10. IBM, Ponemon Institute. Cost of a Data Breach Report 2025. - IBM, 2025.

11. Yuan S., Wu X. Deep learning for insider threat detection: Review, challenges and opportunities // Computers & Security. - 2021. - Vol. 104.

12. Закон Республики Узбекистан от 02.07.2019 г. № ЗРУ-547 «О персональных данных» (с изменениями и дополнениями). - Национальная база данных законодательства (lex.uz).

13. Закон Республики Узбекистан от 15.04.2022 г. № ЗРУ-764 «О кибербезопасности». - URL: https://lex.uz/ru/docs/5960609

14. Указ Президента Республики Узбекистан от 10.03.2026 г. № УП-38 «Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности». - URL: https://lex.uz/ru/doc-passport/8079279

15. UZCERT. Statistics for 2025. - URL: https://uzcert.uz/en/ (дата обращения: 14.11.2026).

16. После кибератаки в Узбекистане утекли 60 тысяч записей, а не данные 15 млн граждан - глава Минцифры // Газета.uz. - 12.02.2026. - URL: https://www.gazeta.uz/ru/2026/02/12/data-leak/

17. Chainalysis. The $6.4 Billion Binance Hack: Tracing the North Korea Link. - 2026. - URL: https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/

18. PHP2Shell: Two Critical PHP Flaws Allow Unauthenticated Remote Code Execution // Security.com. - 22.10.2026. - URL: https://www.security.com/blog-post/php2shell-critical-vulns-cve-2026-109618-109619

19. PHP2Shell: 22M exposed servers at risk as emergency patches released // TechTarget. - 21.10.2026. - URL: https://www.techtarget.com/news/PHP2Shell-22M-exposed-servers-at-risk-as-emergency-patches-released/836071/

20. Хакеры заявили о взломе базы с персональными данными более 27 млн узбекистанцев // Фергана. - Ноябрь 2026. - URL: https://fergana.agency/news/150484/

21. Группировка BUTTERFLY заявила об обнаружении уязвимостей в системах Узбекистана // UzDaily.uz. - Ноябрь 2026. - URL: https://www.uzdaily.uz/ru/gruppirovka-butterfly-zaiavila-ob-obnaruzhenii-uiazvimostei-v-sistemakh-uzbekistana/

22. Knapp E. D., Langill J. T. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2nd ed. - Syngress, 2014.

23. Knapp E. D. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 3rd ed. - Syngress, 2024.

24. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 Revision 2. - NIST, 2015.

25. Radack S. Protecting Industrial Control Systems - Key Components of Our Nation's Critical Infrastructures. ITL Bulletin. - NIST, 2011.